Dr.WEB

Enterprise Security Suite

Managing Linux Workstations

This document is intended for information and reference purposes regarding the Dr.Web software discussed herein. This document is not a basis for exhaustive conclusions about the presence or absence of any functional and/or technical features in Dr.Web software and cannot be used to determine whether Dr.Web software meets any requirements, technical specifications and/or parameters, and other third-party documents.

Trademarks

Disclaimer

In no event shall Doctor Web and its resellers or distributors be liable for any errors or omissions, or for any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, or by the use of or inability to use the information contained in this document.

Dr.Web Enterprise Security Suite. Managing Linux Workstations
Version 13.0
Administrator Manual
12/26/2024

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya, Moscow, Russia, 125124

Website: https://www.drweb.com/

Phone: +7 (495) 789-45-87

Refer to the official website for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web information security solutions that provide effective protection against malicious software and spam.

Doctor Web customers include home users around the world, government agencies, small businesses, and nationwide corporations.

Since 1992, Dr.Web anti-virus solutions have been known for their continuous excellence in malware detection and compliance with international information security standards.

The state certificates and awards received by Dr.Web solutions, as well as the worldwide use of our products, are the best evidence of exceptional trust in the company products.

We thank all our customers for their support and devotion to Dr.Web products!

Table of Contents

1. Introduction

1.1. About This Manual

This manual is a part of documentation package of an anti-virus network administrator and intends to provide detailed information on managing the complex anti-virus protection of corporate computers and mobile devices using Dr.Web Enterprise Security Suite.

The manual is for the anti-virus network administrator—an employee who is responsible for the anti-virus protection of workstations and network servers.

The manual contains the information about centralized configuration of anti-virus software on workstations performed by the anti-virus network administrator via Dr.Web Security Control Center. The manual describes the settings of the Dr.Web Desktop Security Suite anti-virus solution and features of the centralized management of this software.

To get additional information, please refer to the following manuals:

- The Administrator Manual of the Dr.Web Desktop Security Suite anti-virus solution contains information about configuring the anti-virus software directly on a station.
- The Administrator Documentation of the anti-virus network protected by Dr.Web Enterprise Security Suite (includes the Administrator Manual, Installation Manual and Appendices) contains general information on installing and configuring the anti-virus network and, particularly, on using Dr.Web Security Control Center.

Before reading these documents make sure that you have the latest version of the manuals. The manuals are constantly updated and the actual version can always be found at the official website of Doctor Web.

1.2. Conventions and Abbreviations

Conventions

The following symbols and text conventions are used in this guide:

Convention	Comment
❗	An important note or instruction.
⚠	A warning about possible errors or important notes that require special attention.
Anti-virus network	A new term or an emphasis on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Names of keyboard keys.
`/home/user`	Names of files and folders, code examples.
Appendix A	Cross-references to document chapters or internal hyperlinks to webpages.

Abbreviations

The following abbreviations will be used in the Manual without further interpretation:

- CSV—Comma-Separated Values,
- GUI—Graphical User Interface,
- GUS—Dr.Web Global Update System,
- HTML—HyperText Markup Language,
- HTTP—HyperText Transfer Protocol,
- HTTPS—Hypertext Transfer Protocol Secure,
- IP—Internet Protocol,
- LAN—Local Area Network,
- LKM—Linux Kernel Module,
- OS—Operating System,
- PDF—Portable Document Format,
- TCP—Transmission Control Protocol,
- URL—Uniform Resource Locator,

- XML—Extensible Markup Language.

2. Dr.Web Enterprise Security Suite

2.1. About This Product

Dr.Web Enterprise Security Suite is designed for organization and management of integral and reliable complex anti-virus protection of either internal corporate network, including mobile devices, or home computers of employees.

A combination of computers and mobile devices, on which Dr.Web Enterprise Security Suite cooperating components are installed, represents an integral *anti-virus network*.

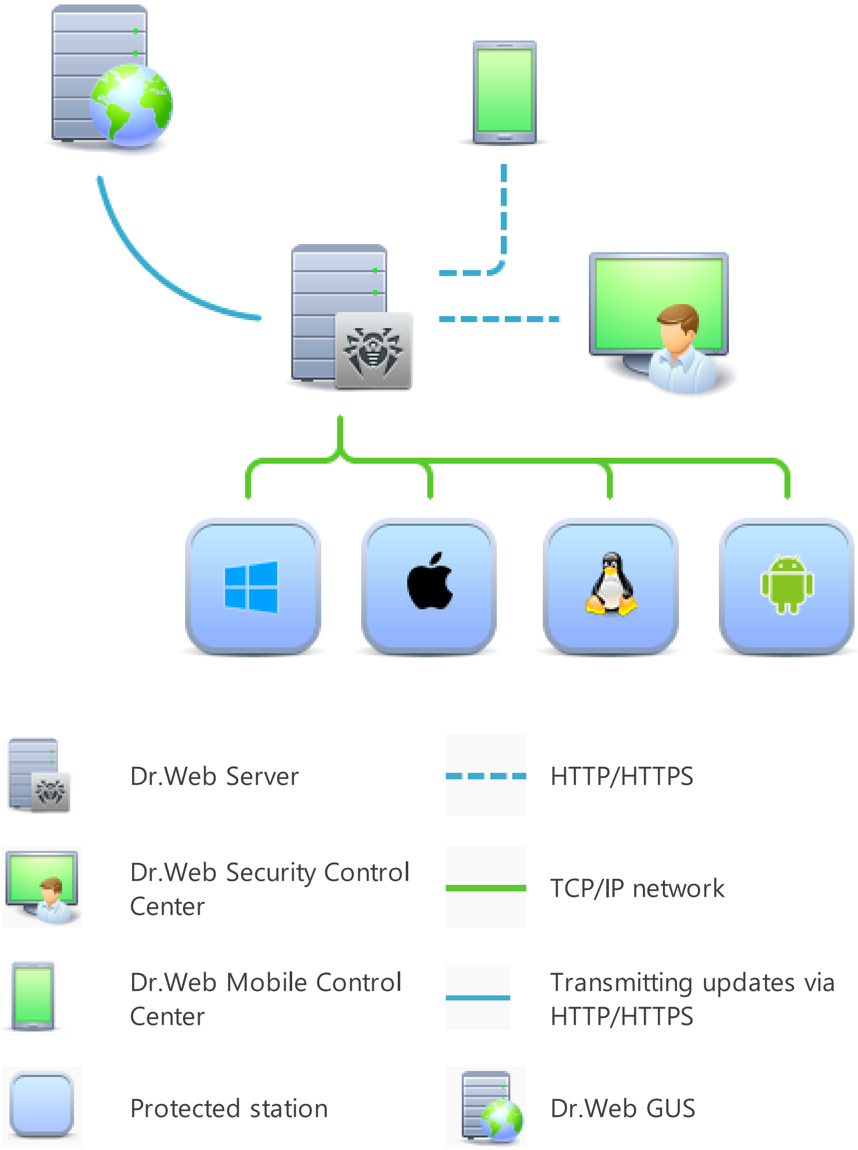
Dr.Web Server
HTTP/HTTPS
Dr.Web Security Control Center
TCP/IP network
Dr.Web Mobile Control Center
Transmitting updates via HTTP/HTTPS
Protected station
Dr.Web GUS

Figure 1. The logical structure of the anti-virus network

The Dr.Web Enterprise Security Suite anti-virus network has a *client-server* architecture. Its components are installed on computers and mobile devices of users and administrators, as well as on computers that function as LAN servers. Anti-virus network components exchange information via TCP/IP. Anti-virus software can be installed on protected stations (and manage them afterwards) either via the LAN, or via the internet.

2.2. Protection of Linux Workstations

Protection of Linux workstations is performed by Dr.Web anti-virus packages.

> The term *anti-virus network station* is used to designate a protected device with the anti-virus package installed.
> This term may refer to a PC, a mobile device or a LAN server.

Anti-virus packages are installed on protected stations and get connected to Dr.Web Server. Each station is included in one or several groups registered on this Server. The protected stations and the Dr.Web Server communicate via the protocol used in the local network (TCP/IP version 4 or 6).

Installation

Local installation is performed on the protected station directly either by the administrator of this station or by the administrator of the anti-virus network.

> For the detailed description of how to install anti-virus packages on protected stations, refer to the Dr.Web Enterprise Security Suite Installation Manual.

Management

When the connection with Dr.Web Server is established, the administrator can use the following functions implemented by the anti-virus package on the protected station:

- Centralized configuration of the anti-virus package on the protected station via the Security Control Center.

  The administrator can either allow or forbid the users to change the settings of the anti-virus package on the protected station.
- Configuring the schedule for anti-virus scans and other tasks to run on the protected station.
- Getting scan statistics and other information on the operation of the anti-virus components and on the state of the protected station.
- Starting and stopping anti-virus scans, etc. (depending on the functionality of the anti-virus package installed on the protected station).

Updating

Dr.Web Server downloads updates and distributes them to the protected stations connected to it. Thus, optimal protection against threats is implemented, maintained and adjusted automatically regardless of the skills of the administrator of the protected stations.

If a protected station is disconnected from the anti-virus network, the anti-virus package installed on the server uses the local copy of the settings and the anti-virus protection retains its functionality (until the expiration of the user license), but the software is not updated. If the protected station is allowed to use the *Mobile mode*, the virus bases can be updated directly from Dr.Web GUS servers after the connection with Dr.Web server is lost.

> The operation of the stations in the mobile mode is described in Chapter 4 of this Manual.

3. Dr.Web Desktop Security Suite

3.1. Dr.Web Desktop Security Suite Functions

This Manual describes aspects of configuring components of Dr.Web Desktop Security Suite designed for GNU/Linux. The Manual is intended for a person responsible for anti-virus protection and configuration of networks (hereinafter referred to as "Administrator").

Dr.Web Desktop Security Suite is designed to protect workstations running on OSes of GNU/Linux family from viruses and other types of malicious software, and to prevent distribution of threats designed for different platforms.

Main features of Dr.Web Desktop Security Suite:

1. **Detection and neutralization of threats.** Scans for malicious programs of all possible types (various viruses, including those that infect mail files and boot records, trojans, mail worms, and so on) and unwanted software (adware, joke programs and dialers).

   Threat detection methods:

   - *signature analysis*—a scan method allowing to detect known threats registered in virus databases;
   - *heuristic analysis*—a set of scan methods allowing to detect threats that are not known yet;
   - *using Dr.Web Cloud* service, which collects up-to-date information about recent threats and sends it to various products of Doctor Web.

   Note that the heuristic analyzer may raise false-positive detections of legitimate software. Thus, objects that contain threats detected by the analyzer are considered “suspicious”. It is recommended that you choose to quarantine such files and send them for analysis to the Doctor Web anti-virus laboratory.

   Scanning the file system at user request can be performed in two modes: full scan (scanning all file system objects) and custom scan (scanning selected objects—directories or files that satisfy specified criteria). Moreover, the user can start a separate scan of volume boot records and executables that spawned currently active processes. In the latter case, if a malicious executable is detected, it is neutralized and all processes spawned by this file are forced to terminate.

2. **Monitoring file access.** Data file events and attempts to run executables are monitored. This feature allows to detect and neutralize malware instantly at attempt of infecting the computer.

3. **Monitoring access to the internet.** Attempts to access internet servers (web, mail and file servers) are monitored to block access to websites from the unwanted categories, and to prevent receiving and sending of email messages with infected files, unwanted links or spam. Scanning email messages and files downloaded from the internet for viruses and other threats is performed “on-the-fly”. To determine unwanted links, Dr.Web Desktop Security Suite is bundled with an automatically updated database of web resource categories and black and white lists that are manually edited by the user. The Dr.Web Cloud

service is also used to check whether a web resource requested by the user is marked malicious by other anti-virus products of Doctor Web.

4. **Reliable isolation of infected or suspicious objects** in a special storage (quarantine) to prevent any harm to the system. When quarantined, objects are renamed according to custom rules and, if necessary, they can be restored to their original location only on demand of the user.

3.2. Dr.Web Desktop Security Suite Components

For the protection of Linux workstations, the following components are provided:

General

Scanner for Workstations

The component which performs scanning of file system objects (files, directories, and boot records) and running processes on user's demand or on schedule to detect threats.

Note that the GUI version of the Scanner is meant by the Scanner for Workstations. Dr.Web Desktop Security Suite also comprises the Console Scanner that is used to run scan from a command line. The Control Center does not manage the Console Scanner operation.

SpIDer Guard (for GNU/Linux version)

A GNU/Linux file system monitor. Operates in a background mode and controls file operations (such as creation, opening, closing, running). Sends requests to File Checker to scan new and modified files, as well as executables upon starting programs.

SpIDer Gate

A component for scanning network traffic and URLs. It is designed for scanning for threats all data downloaded to a local host from the network and sent from it to an external network. The component prevents from connecting to network hosts covered by the unwanted categories of web resources and black lists created by the system administrator.

The component is supplied only with the distributions designed for GNU/Linux OSes.

Console Scanner

A component allowing to start scanning files on a workstation from the command line.

Dr.Web ClamD

A component emulating interface of ClamAV® anti-virus product. Enables all applications that support ClamAV® to use Dr.Web Desktop Security Suite for anti-virus scanning.

Quarantine

Used by the Scanner for Workstations, Console Scanner and SpIDer Guard for isolating malicious and suspicious objects.

Auxiliary

Dr.Web Agent for Unix

An auxiliary component. Used for interaction of Dr.Web Desktop Security Suite installed on the station with Dr.Web Enterprise Security Suite.

File Checker

Used by the Console Scanner to pass files to the Scanning Engine for scanning and to manage Quarantine on the station.

Network Checker

Used to pass data sent over the network by the components of the software suite to Scanning Engine for scanning. The component is used by all general components.

Scanning Engine

Used by File Checker and Network Checker for anti-virus scan and virus database management.

SNMP Agent

The component is designed for integration of Dr.Web Desktop Security Suite with external monitoring systems via the SNMP protocol.

Dr.Web ConfigD

Coordinates operation of all Dr.Web Desktop Security Suite components.

Dr.Web CloudD

A component receiving information from the cloud service about whether visited URLs and transferred files are dangerous.

Dr.Web HTTPD

A web server for managing Dr.Web Desktop Security Suite components. Provides the management web interface.

3.3. Dr.Web Desktop Security Suite Operation Modes

Dr.Web Desktop Security Suite can operate both in a standalone mode and as a part of an *anti-virus network* managed by a *centralized protection server*. Such operation mode is called *centralized protection mode*. Using this mode does not require installation of additional software or Dr.Web Desktop Security Suite re-installation or uninstallation.

- In a *standalone mode*, the protected computer is not connected to the anti-virus network and its operation is managed locally. In this mode, configuration and license key files are located on local disks and Dr.Web Desktop Security Suite is fully controlled from the protected computer. Updates of virus databases are received from Doctor Web update servers.
- In the *centralized protection mode*, protection of the computer is managed by the centralized protection server. In this mode, some functions and settings of Dr.Web Desktop Security Suite can be adjusted or locked in accordance with the general (corporate) anti-virus protection policy implemented on the anti-virus network. A custom license key file received from a selected centralized protection server to which Dr.Web Desktop Security Suite is connected is used on the computer in this mode. A license or demo key file stored on the local computer, if any, is not used. The information about Dr.Web Desktop Security Suite operation, including statistics on virus events, is sent to the centralized protection server. Updates of virus databases are also received from the centralized protection server.
- In the *mobile mode*, Dr.Web Desktop Security Suite receives updates from Doctor Web update servers, but uses settings stored locally and a custom license key file that were received from the centralized protection server.

When Dr.Web Desktop Security Suite is operating in the centralized protection mode or the mobile mode, the following options are blocked:

1. Deletion of a license key file in License Manager.
2. Manual start of an update process and adjustment of update settings.
3. Configuration of file system scanning parameters.

Configuration of SpIDer Guard settings, as well as an option to enable or disable it while Dr.Web Desktop Security Suite is running under control of the centralized protection center, are dependent on permissions specified on the server.

In the centralized protection mode, scanning files according to a set schedule is not available.

Note that if starting scanning on demand is prohibited on the centralized protection server, the page for starting scanning and the **Scanner** button from the Dr.Web Desktop Security Suite window will be disabled.

Centralized Protection Concept

Doctor Web solutions for managing centralized protection use a client-server model (see the figure below).

Corporate computers or computers of users of an IT service provider are protected by *local anti-virus components* (in this case, of Dr.Web Desktop Security Suite), which ensure anti-virus protection and maintain connection to the centralized protection server.

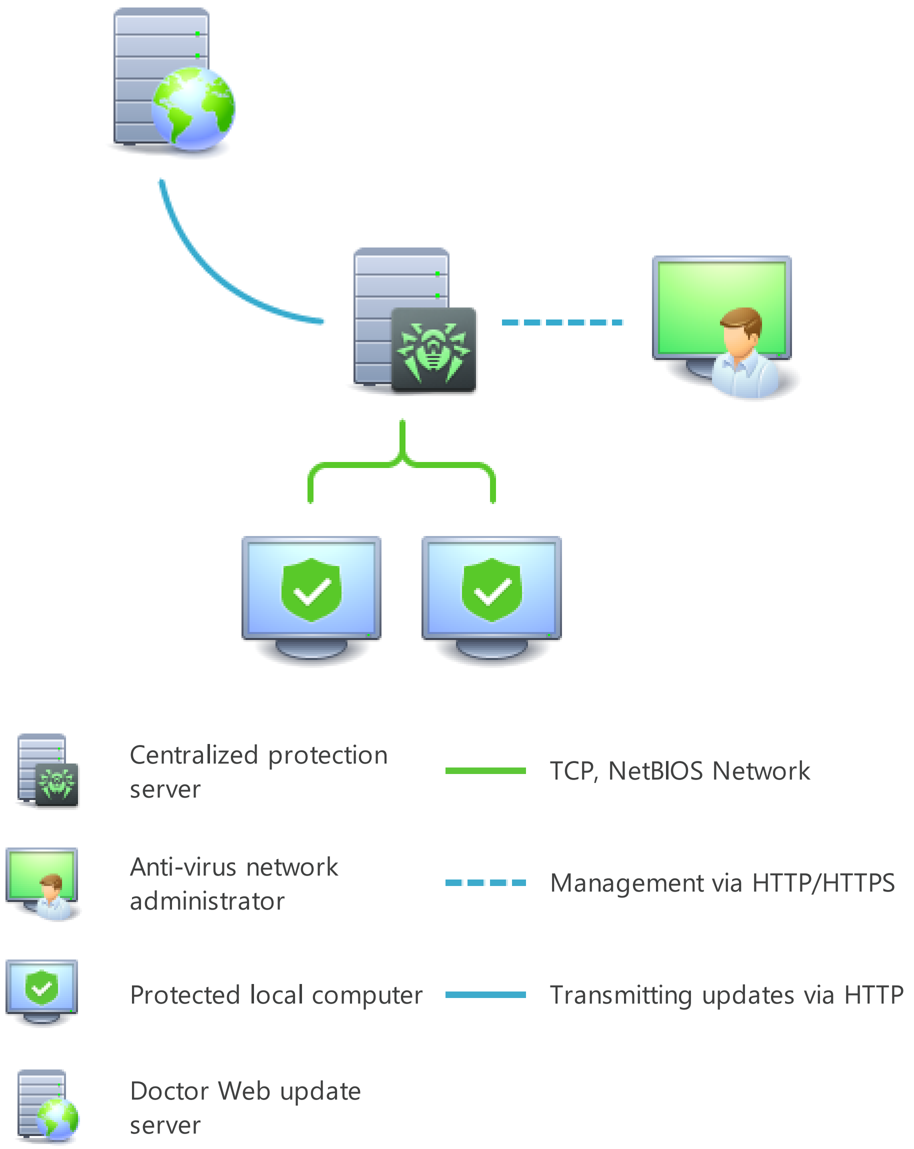
Centralized protection server
TCP, NetBIOS Network
Anti-virus network administrator
Management via HTTP/HTTPS
Protected local computer
Transmitting updates via HTTP
Doctor Web update server

Figure 2. The logical structure of the anti-virus network

Local computers are updated and configured from the *centralized protection server*. The entire stream of instructions, data and statistics in the anti-virus network passes the centralized protection server. The volume of traffic between protected computers and the centralized protection server can be significant, therefore an option for traffic compression is provided.

Using encryption while transmitting data prevents leak of sensitive data or substitution of software downloaded to protected computers.

All necessary updates are downloaded to the centralized protection server from Doctor Web update servers.

Changes in the configuration of local anti-virus components and command transfer are performed by anti-virus network administrators using the centralized protection server. The administrators manage configuration of the centralized protection server and topology of the anti-virus network (for example, they validate connection of a local station to the network) and configure operation of individual local anti-virus components when necessary.

⚠ Local anti-virus components are not compatible with anti-virus products of other companies or Dr.Web anti-virus solutions if the latter do not support operation in the centralized protection mode (for example, Dr.Web for Linux version 5.0). Installation of two anti-virus programs on the same computer can cause a system crash and loss of important data.

Dr.Web Desktop Security Suite version 11.1 operating in the centralized protection mode is compatible with Dr.Web Enterprise Security Suite of versions 11, 12, 13 and 13.0.1.

The centralized protection mode allows exporting and saving Dr.Web Desktop Security Suite operation reports using the centralized protection center. Reports can be exported and saved in the following formats: HTML, CSV, PDF, and XML.

Connecting to the Anti-Virus Network

Dr.Web Desktop Security Suite can be connected to the anti-virus network in one of the following ways:

- On the **Mode** tab of the Dr.Web Desktop Security Suite configuration page.
- Using the `esconnect` command of the `drweb-ctl` command-line management tool.

Disconnecting From the Anti-Virus Network

Dr.Web Desktop Security Suite can be disconnected from the anti-virus network in one of the following ways:

- On the **Mode** tab of the Dr.Web Desktop Security Suite configuration page.
- Using the `esdisconnect` command of the `drweb-ctl` command-line management tool.

3.4. Dr.Web Desktop Security Suite Configuration

To view or edit the settings of the anti-virus components on a workstation:

1. Choose **Anti-virus network** in the main menu of the Control Center.
2. In the hierarchical list of the opened window, click the name of a station under the required OS (GNU/Linux) or a group comprising such stations.
3. In the **Configuration** section of the opened control menu, in the required OS subsection (GNU/Linux), choose the necessary component.
4. A window with the anti-virus component settings will open.

   Managing settings of anti-virus components via the Control Center differs from managing settings directly via the corresponding components on a station:

   - to manage individual parameters, use buttons located on the right from the corresponding settings:

     Reset to initial value—restore a value assigned to the parameter before editing (the latest saved value);

     Reset to default value—reset the parameter to the default value;

   - to manage a set of parameters, use buttons located on the toolbar:

     Reset all parameters to initial values—restore values assigned to the parameters of this section before editing (the latest saved values);

     Reset all parameters to default values—reset all parameters in this section to default values;

     Propagate these settings to another object—copy the settings from this section to the settings of another station or group, or multiple groups or stations.

     Set inheritance of settings from primary group—remove individual settings of the station and inherit the settings of this section from the primary group.

     Copy settings from primary group and set them as personal—copy the settings of this section from the primary group and set them for the selected stations. In this case inheritance is not set and the settings of the station are considered individual.

     Export settings from this section to the file—save all settings from this section to a file in a specific format.

     Import settings to this section from the file—replace all settings in this section with the settings from the file in the specific format.

5. After you have changed any settings via the Control Center, click **Save** to accept the changes. The settings will be passed to the stations. If the stations are offline when changes are made, the settings will be passed when they connect to the Server.

   The administrator may prevent a user from editing settings on a station (see the section **Permissions of Station Users** in the Administrator Manual). Moreover, only the administrator will be able to edit settings via the Control Center.

3.4.1. Scanner for Workstations

Dr.Web Scanner runs an express or full scan of the entire file system or scans critical files and directories only.

Dr.Web Scanner settings for computers running operating systems of the GNU/Linux family are available in the **Scanner for workstations** section. This section allows to adjust the settings of the GUI version of Dr.Web Scanner. Console scanner settings are managed locally on the station.

General

On the **General** tab, you can configure general parameters of Dr.Web Scanner operation.

- In the **Scanning time of one element** field, specify the time limit for scanning a file. Value 0 means that the time period to scan one file is unlimited.

> ⚠ Scanning the contents of archives and email files and increasing the time limit for scanning a single file may slow down the system and increase the overall scanning time.

Actions

In this section, you can configure actions that will be applied to threats detected by Dr.Web Scanner. The actions are set separately for each type of malicious and suspicious objects. These actions vary for different object types.

Dr.Web Scanner can react to the following threats:

- **Infected**—the scanned file contains a known threat;
- **Suspicious**—the scanned file has been marked as *suspicious*;
- **Adware**—the scanned file contains adware;
- **Dialers**—the scanned file contains a dialer;
- **Jokes**—the scanned file contains a joke program;
- **Riskware**—the scanned file contains riskware;
- **Hacktools**—the scanned file contains a hacktool.

Available actions:

- **Cure, move to quarantine if not cured**—restore the state of the object before the infection. If the object is incurable or the attempt of curing fails, the object is quarantined.

  This action is available only for the objects infected with a known virus that can be cured except for trojans and infected files within compound objects (archives, email files or file containers).

- **Cure, delete if not cured**—restore the state of the object before the infection. If the object is incurable or the attempt of curing fails, the object is deleted.

This action is available only for the objects infected with a known virus that can be cured except for trojans and infected files within compound objects (archives, email files or file containers).

- **Delete**—delete the object that poses a threat.

  This is the most effective way to remove all types of threats.
- **Move to quarantine**—move a detected threat to a special directory isolated from the rest of the system.
- **Report**—notify of a threat without performing other actions.

> Default settings are optimal in most cases. Do not change them unless necessary.

Choose **Automatically apply actions to threats** to automatically apply actions indicated above to threats detected during scanning. If this option is disabled, the user will be notified about a detected threat, but no actions to neutralize it will be taken.

You can also disable scanning archives and email files. This option is enabled by default.

Table 1. Actions applied to threats detected by Dr.Web Scanner

Object	Action				
	Cure, move to quarantine incurable	Cure, delete incurable	Delete	Move to quarantine	Report
Infected	+/*	+	+	+	
Suspicious			+	+/*	+
Adware			+	+/*	+
Dialers			+	+/*	+
Jokes			+	+	+/*
Riskware			+	+	+/*
Hacktools			+	+	+/*

Conventions

+	action is enabled for an object of this type
+/*	action is set as default for an object of this type

Excluded paths

In this area, specify paths to files and directories that will be excluded from scanning by Dr.Web Scanner.

3.4.2. SpIDer Guard Settings

3.4.2.1. General Settings

On this page you can manage the following parameters of SpIDer Guard on the protected station (file server):

- **Enable SpIDer Guard for Linux**—enable or disable SpIDer Guard on the protected station.
- **Use heuristic analysis**—define how SpIDer Guard uses the heuristic analysis on the protected station while scanning files “on-the-fly”. The heuristic analysis slows down scanning, but improves its reliability.
- **Scanning time of one element**—set a time limit for scanning one file by SpIDer Guard on the station. If the value is set to *0*, the time period for scanning one file is unlimited.

> The SpIDer Guard file system monitor can operate in one of these two modes:
>
> - `FANOTIFY`—using the `fanotify` system mechanism (not all GNU/Linux OSes support this mode);
> - `LKM`—using the loadable Linux kernel module (can be used in any GNU/Linux OS with kernel 2.6.x and later).
>
> By default, the file system monitor automatically chooses the appropriate operation mode according to the environment. If SpIDer Guard cannot be started, build and install the loadable kernel module on the protected station using the supplied source code.

3.4.2.2. Actions

On this page you can manage anti-virus protection parameters used by SpIDer Guard to scan files.

SpIDer Guard can react to the following threats:

- **Infected**—the scanned file contains a known threat;
- **Suspicious**—the scanned file has been marked as *suspicious*;
- **Adware**—the scanned file contains adware;
- **Dialers**—the scanned file contains a dialer;
- **Jokes**—the scanned file contains a joke program;
- **Riskware**—the scanned file contains riskware;

- **Hacktools**—the scanned file contains a hacktool.

Available actions:

- **Cure, move to quarantine if not cured**—restore the state of the object before the infection. If the object is incurable or the attempt of curing fails, the object is quarantined.

  This action is available only for the objects infected with a known virus that can be cured except for trojans and infected files within compound objects (archives, email files or file containers).
- **Cure, delete if not cured**—restore the state of the object before the infection. If the object is incurable or the attempt of curing fails, the object is deleted.

  This action is available only for the objects infected with a known virus that can be cured except for trojans and infected files within compound objects (archives, email files or file containers).
- **Delete**—delete the object that poses a threat.

  This is the most effective way to remove all types of threats.
- **Move to quarantine**—move a detected threat to a special directory isolated from the rest of the system.
- **Report**—notify of a threat without performing other actions.

> Default settings are optimal in most cases. Do not change them unless necessary.

Table 2. Actions applied to threats detected by Dr.Web SpIDer Guard

Object	**Action**				
	Cure, move to quarantine incurable	**Cure, delete incurable**	**Delete**	**Move to quarantine**	**Report**
Infected	+/*	+	+	+	
Suspicious			+	+/*	+
Adware			+	+/*	+
Dialers			+	+/*	+
Jokes			+	+	+/*
Riskware			+	+	+/*
Hacktools			+	+	+/*

Conventions

+	action is enabled for an object of this type

+/*	action is set as default for an object of this type

3.4.2.3. Containers

On this page you can manage settings used by SpIDer Guard for scanning compound files, such as archives, mail files, packed objects and other containers (i.e. the compound files that are not related to any of the types above).

You can specify the nesting level limit for each of the file types in the corresponding field; when this limit is exceeded, SpIDer Guard will not unpack a file of such type during scanning. For example, to scan the contents of the archives that are nested in archives, specify the nesting level limit of no less than *2*. To disable scanning of nested objects, specify *0* as the maximum nesting level for the corresponding type of containers.

Note that increasing the maximum nesting level slows down scanning.

The **Maximum compression ratio** field allows you to specify the maximum compression ratio (as a compressed/uncompressed file ratio) for objects to be scanned. If the compression ratio of an object to be scanned exceeds the specified value, this object will not be scanned.

3.4.2.4. Scanning Paths

On this page you can manage a list of paths to files and directories on the protected station to be scanned or skipped by SpIDer Guard while monitoring the file system.

Excluded paths are specified in the **Excluded paths** field (one path per line). Files and directories added to the list of the excluded paths are skipped by the SpIDer Guard monitor.

The excluded processes are specified in the **Excluded processes** field (one process per line). All file actions performed by processes (programs) from this list are not monitored by SpIDer Guard. For each process to be excluded it is necessary to specify a full executable path on the protected station.

The paths to be scanned on the protected station are specified in the **Scanned paths** field (one path per line). The SpIDer Guard monitor controls only those files that are added to the scanned paths and does not control those added to the paths from the **Excluded paths** list.

To add a new path to the relevant list, click + in the corresponding row of the list. To remove a path from the list, click − in the corresponding row of the list.

3.4.2.5. Advanced Settings

On this page you can manage advanced SpIDer Guard settings on the protected station (file server).

The following advanced SpIDer Guard settings are available:

- **Operation mode**—set one of the operation modes for SpIDer Guard on the protected station: using the Linux kernel module (LKM), using the fanotify system service, or in an auto mode, when a suitable operation mode is detected automatically. It is recommended to keep the *AUTO* value.
- **Log level**—a log verbosity level used for SpIDer Guard message logging.
- **Logging method**—a logging method for SpIDer Guard. The following values are allowed:
    - *Auto*—use logging parameters defined for all components in Dr.Web ConfigD settings.
    - *Syslog*—use the syslog system service for SpIDer Guard message logging. If you choose this method, you must also specify a value of the **Syslog facility** parameter in the drop-down list. This parameter defines a subsystem (label) to be used by syslog to store messages from SpIDer Guard.
    - *Path*—use a separate file to store SpIDer Guard log messages. If you choose this method, you must also specify a path to the file in the **Log file** field.

3.4.3. Dr.Web Agent for Unix Settings

3.4.3.1. General Settings

On this page you can manage the following settings of the auxiliary component Dr.Web Agent for Unix on the protected station:

- **Collect information about stations**—allow or do not allow Dr.Web Agent for Unix to collect statistics about stations.
- **Period of collecting information about stations**—specify the frequency (in minutes) with which Dr.Web Agent for Unix should send requests to stations to collect information.
- **Statistics sending period**—set the frequency with which Dr.Web Agent for Unix should send statistics to the server.
- **Mobile mode for updates**—set up the mobile mode for updates. The following values are allowed:
    - *Auto*—use the mobile mode, if allowed by the administrator of the Dr.Web Enterprise Security Suite server (fetch updates either from GUS servers by using a local updating component installed on the station, or fetch updates from Dr.Web Enterprise Security Suite, depending on which connection is available and which the quality of which connection is better).
    - *Enable*—use the mobile mode, if allowed by the administrator of the Dr.Web Enterprise Security Suite server (fetch updates from GUS servers using a local updating component installed on the station).
    - *Disable*—do not allow Dr.Web Desktop Security Suite installed on the station to fetch updates from GUS servers in case of a failure to connect to the Dr.Web Enterprise Security Suite server.

- **Process discovery requests**—select the check box to allow the agent to receive discovery requests (used to check the structure and state of the anti-virus network) from the Dr.Web Enterprise Security Suite server.
- **Log level**—a log verbosity level used for Dr.Web Agent for Unix message logging.
- **Logging method**—a logging method for Dr.Web Agent for Unix. The following values are allowed:
    - *Auto*—use logging parameters defined for all components in Dr.Web ConfigD settings.
    - *Syslog*—use the syslog system service for Dr.Web Agent for Unix message logging. If you choose this method, you must also specify a value of the **Syslog facility** parameter in the drop-down list. This parameter defines a subsystem (label) to be used by syslog to store messages from Dr.Web Agent for Unix.
    - *Path*—use a separate file to store Dr.Web Agent for Unix log messages. If you choose this method, you must also specify a path to the file in the **Log file** field.

⚠ Usually, default values specified for the parameters of this component are optimal. Thus, it is not recommended to change them unless necessary.

3.4.3.2. Configuration

On this page you can specify settings for any of the Dr.Web Desktop Security Suite components installed on the station (an `.ini` configuration file format is used). For that, introduce required changes to the **drweb.ini configuration file** field.

Note that:

- The Control Center does not support configuring all existing parameters. To configure Dr.Web Agent for Unix components in depth, use the Dr.Web Desktop Security Suite configuration editor.
- The settings editor shows only those configuration parameters the values of which have been changed on this page.
- The values of the configuration parameters specified in the editor take precedence over the values specified by component configuration pages: if a value of some parameter is specified on a configuration page and a different value is specified on the **Configuration** page, the value specified on the **Configuration** page will be used for the station. Moreover, undefined configuration parameters take default values for components which sections are provided in the **drweb.ini configuration file** editor.
- The configuration editor supports context help: to show a drop-down list of available parameters (or parameter sections, depending on the context), press CTRL+SPACE.
- You can import and export editor contents as an `.ini` configuration file. To do that, click the corresponding button on the page above the configuration editor.

ⓘ For the complete list of components on the station that are available for configuration, and for description of their parameters provided in the `drweb.ini` configuration file, refer to the User manual or the Administrator manual for the product installed on the station.

3.4.4. SpIDer Gate Settings

3.4.4.1. General Settings

On this page you can manage the following parameters of SpIDer Gate on the protected station:

- **Run SpIDer Gate**—enable or disable SpIDer Gate on the protected station.
- **Use heuristic analysis**—define how SpIDer Gate uses the heuristic analysis on the protected station to detect unknown threats. The use of the heuristic analysis slows down scanning but improves its reliability.
- **Scanning time of one element**—set a time limit for scanning one file by SpIDer Guard on the station. If the value is set to *0*, the time period for scanning one file is unlimited.

3.4.4.2. Actions

On this page you can manage the following parameters of SpIDer Gate on the protected station:

- Set the **Scan received files** check box to enable scanning incoming internet traffic (in particular, files downloaded from the internet).
- In the **Block files** and **Additionally block** sections, select types of incoming malicious objects to be blocked by SpIDer Gate.

3.4.4.3. Web Filtering

On this page you can manage the following parameters of SpIDer Gate on the protected station:

- Select the **Scan URL** check box to block internet resources by categories.
- Select the **Block non-recommended websites** check box to block access to websites that use social engineering techniques to misguide users.
- Select the **Block URLs listed due to a notice from copyright owner** check box to block access to websites due to a notice from copyright owners who have discovered a violation of their rights to intellectual property on the internet.
- In the **Block websites from the following categories** section, choose categories of websites to block access to.
- In the **White list/Black list** sections, add paths to websites to be allowed/blocked:
  - To add a certain website, enter its full domain address (for example, `www.example.com`). Access to all resources of this domain will be defined by this string.

3.4.4.4. Containers

On this page you can manage settings used by SpIDer Gate for scanning compound files, such as archives, mail files, packed objects and other containers (i.e. the compound files that are not related to any of the types above).

You can specify the nesting level limit for each of the file types in the corresponding field; when this limit is exceeded, SpIDer Gate will not unpack a file of such type during scanning. For example, to scan the contents of the archives that are nested in archives, specify the nesting level limit of no less than *2*. To disable scanning of nested objects, specify *0* as the maximum nesting level for the corresponding type of containers.

Note that increasing the maximum nesting level slows down scanning.

The **Maximum compression ratio** field allows you to specify the maximum compression ratio (as a compressed/uncompressed file ratio) for objects to be scanned. If the compression ratio of an object to be scanned exceeds the specified value, this object will not be scanned.

3.4.4.5. Advanced Settings

On this page you can manage advanced SpIDer Gate settings on the protected station.

The following advanced SpIDer Gate settings are available:

- **Log level**—a log verbosity level used for SpIDer Gate message logging.
- **Logging method**—a logging method for SpIDer Gate. The following values are allowed:
  - *Auto*—use logging parameters defined for all components in Dr.Web ConfigD settings.
  - *Syslog*—use the syslog system service for SpIDer Gate message logging. If you choose this method, you must also specify a value of the **Syslog facility** parameter in the drop-down list. This parameter defines a subsystem (label) to be used by syslog to store messages from SpIDer Gate.
  - *Path*—use a separate file to store SpIDer Gate log messages. If you choose this method, you must also specify a path to the file in the **Log file** field.

3.4.5. File Checker Settings

On this page you can manage settings used by the File Checker auxiliary component on the protected station.

The following settings are available:

- **Maximum checked file cache size**—a size of the cache used by File Checker to temporarily store file scan results.
- **Cache validity period**—a time period during which File Checker does not rescan files, if scan results are already available in the cache.

- **Log level**—a log verbosity level used for File Checker message logging.
- **Logging method**—a logging method for File Checker. The following values are allowed:
  - *Auto*—use logging parameters defined for all components in Dr.Web ConfigD settings.
  - *Syslog*—use the syslog system service for File Checker message logging. If you choose this method, you must also specify a value of the **Syslog facility** parameter in the drop-down list. This parameter defines a subsystem (label) to be used by syslog to store messages from File Checker.
  - *Path*—use a separate file to store File Checker log messages. If you choose this method, you must also specify a path to the file in the **Log file** field.

Moreover, you can choose which additional data will be stored in the log at the *Debug* verbosity level.

- **IPC**—log all inter-process communication (IPC) messages on component interaction.
- **File scanning**—log info about file scans.
- **SpIDer Guard file monitoring**—log SpIDer Guard scan requests.
- **Checked file cache status**—log status information about the cache for scanned files.

> ⚠ Usually, default values specified for the parameters of this component are optimal. Thus, it is not recommended to change them unless necessary.

3.4.6. Scanning Engine Settings

On this page you can manage settings used by the Scanning Engine auxiliary component on the protected station.

The following settings are available:

- **Path to the socket file of the fixed copy of the component**—a path to a Unix socket file of a resident Scanning Engine instance. This socket can be used to scan files by external programs. If the parameter is empty, scanning files is unavailable to external programs, and Scanning Engine runs and terminates automatically, when necessary.
- **Number of scanning processes**—a number of child scanning processes that can be created by Scanning Engine while scanning files. When changing the value of this parameter, take into account the number of CPU cores available on the station.
- **Watchdog timer**—a time period used by Scanning Engine to automatically detect a hang-up of child scanning processes.
- **Log level**—a log verbosity level used for Scanning Engine message logging.
- **Logging method**—a logging method for Scanning Engine. The following values are allowed:
  - *Auto*—use logging parameters defined for all components in Dr.Web ConfigD settings.
  - *Syslog*—use the syslog system service for Scanning Engine message logging. If you choose this method, you must also specify a value of the **Syslog facility** parameter in the drop-

down list. This parameter defines a subsystem (label) to be used by syslog to store messages from Scanning Engine.

- *Path*—use a separate file to store Scanning Engine log messages. If you choose this method, you must also specify a path to the file in the **Log file** field.

⚠ Usually, default values specified for the parameters of this component are optimal. Thus, it is not recommended to change them unless necessary.

3.4.7. Dr.Web ConfigD Settings

On this page you can manage parameters that are used by the Dr.Web ConfigD auxiliary management component during its operation on the protected station.

The following settings are available:

- **Public communication socket path**—a path to a Unix socket used by Dr.Web Desktop Security Suite components for interaction with Dr.Web ConfigD.
- **Administrative communication socket path**—a path to a Unix socket used by Dr.Web Desktop Security Suite components operating with superuser privileges for interaction with Dr.Web ConfigD.
- **Temporary files directory**—a path to a directory with temporary files stored by Dr.Web Desktop Security Suite components.
- **Path to the directory with PID files and communication sockets**—a path to a directory with PID files and Unix sockets that are used for internal interaction of Dr.Web Desktop Security Suite components.
- **Log level**—a log verbosity level used for Dr.Web ConfigD message logging.
- **Logging method**—a logging method for Dr.Web ConfigD. The following values are allowed:
  - *Syslog*—use the syslog system service for Dr.Web ConfigD message logging. If you choose this method, you must also specify a value of the **Syslog facility** parameter in the drop-down list. This parameter defines a subsystem (label) to be used by syslog to store messages from Dr.Web ConfigD.
  - *Path*—use a separate file to store Dr.Web ConfigD log messages. If you choose this method, you must also specify a path to the file in the **Log file** field.

⚠ Usually, default values specified for the parameters of this component are optimal. Thus, it is not recommended to change them unless necessary.

4. Updating Mobile Dr.Web Agents

General Information

If a user workstation has no access to Dr.Web Server for a long time, Dr.Web Agent on the station can get updates from Dr.Web GUS servers in the *mobile mode*. The mobile mode must be activated on the station and also permitted on the server.

You can set the mobile mode settings by changing the value of the `EsAgent.MobileMode` parameter:

```
# drweb-ctl cfset EsAgent.MobileMode <required value>
```

This parameter can have the following values:

- *on*—use the mobile mode only (if permitted on the server) and get updates only from the Dr.Web GUS servers;
- *off*—do not use the mobile mode and get updates only from the centralized protection server;
- *auto*—use the mobile mode (if permitted on the server) and get updates either from the Dr.Web GUS servers or from the centralized protection server (depending upon which connection is available and which connection has a better quality).

Operation in the Mobile Mode with Default Settings

The *auto* value is set by default. The station will get updates from the Dr.Web GUS servers in the following cases:

- no updates have been received successfully from the centralized protection server during 24 hours;
- the connection to the centralized protection server cannot be established during 10 minutes.

In the mobile mode the Dr.Web Agent tries to connect to the centralized protection server once a minute. If the connection is kept for 10 minutes after a successful attempt, updates from the centralized protection server will be available again.

5. Appendix A. Technical Support

If you have a problem installing or using Doctor Web products, please try the following before contacting technical support:

1. Download and review the latest manuals and guides at https://download.drweb.com/doc/.
2. See the Frequently Asked Questions section at https://support.drweb.com/show_faq/.
3. Browse the official Doctor Web forum at https://forum.drweb.com/.

If you haven't found a solution to your problem, you can request direct assistance from Doctor Web technical support specialists. Please use one of the options below:

1. Fill out a web form in the appropriate section at https://support.drweb.com/.
2. Call +7 (495) 789-45-86 (for customers in Moscow) or 8-800-333-79-32 (a toll-free line for customers within Russia).

For information on regional and international offices of Doctor Web, please visit the official website at https://company.drweb.com/contacts/offices/.